VPN 클라이언트에서 보안 클라이언트 RAVPN 스플릿 터널/기본 DNS에 대한 IP 전달 테이블 수정 오류를 성공적으로 확인할 수 없음(&n)

목차

문제

Mac 사용자는 Cisco Secure Client VPN에 연결되어 있는 동안 내부 응용 프로그램에 CLI 인증을 시도할 때 간헐적인 오류가 발생합니다. 이 오류는 CLI 인증 도중 및 `curl`과 같은 명령을 사용할 때 "host not found(호스트를 찾을 수 없음)" 오류로 나타납니다. 그러나 nslookup 및 `dig`와 같은 DNS 확인 명령은 성공합니다. 이 문제는 무작위로 발생하며 VPN을 다시 연결하여 일시적으로 해결할 수 있습니다. 이 경우 문제가 다시 발생하기 전에 잠시 연결이 작동합니다. 스플릿 터널 VPN이 사용 중이며 Cisco Umbrella가 활성 상태입니다. Palo Alto GlobalProtect VPN을 사용할 때는 문제가 발생하지 않습니다.

- 오류 메시지: CLI 인증 및 curl 명령에 "host not found"가 있습니다.
- 오류 메시지: VPN 클라이언트에서 IP 전달 테이블 수정을 확인할 수 없습니다. 개인 리소스를 연결하는 동안 DNS(Domain Name Server) 확인 문제가 발생했습니다
- `nslookup` 및 `dig` 명령 성공
- VPN 재연결 후 간헐적 연결
- 스플릿 터널 원격 액세스 VPN 및 Umbrella 모듈 사용
- MacOS 디바이스에서 Cisco Secure Client VPN에서만 재현할 수 있는 문제

환경

- 제품: 여러 모듈이 포함된 Cisco CSC(Secure Client)
- 플랫폼: 기업 Mac 장치
- VPN 프로필 구성: 원격 액세스 VPN 프로필 - 보안 액세스 우회 - 스플릿 터널 모드 및 "기본 DNS"로 선택된 DNS 모드
- DNS 필터링: Cisco Umbrella 활성화
- 모듈 버전:
    - 클라우드 관리 v1.0.0.23
    - AnyConnect VPN v5.1.13.177
    - 우산 v5.1.13.177
    - DART v5.1.13.177
    - 보안 방화벽 상태 v5.1.13.177
    - 네트워크 가시성 모듈 v5.1.13.177
- 진단 데이터: 분석을 위해 수집된 DART 번들
- Cisco Secure Client VPN에서만 관찰됨(Palo Alto GlobalProtect 제외)

해결

- 클라이언트 측에서 VPN 프로파일(naic.org) 스플릿 터널 구성 및 AnyConnect VPN 라우팅 테이블을 디버깅하는 동안 다음 동작이 관찰되었습니다.
  - 작업 시나리오 - Vault 비제품 로컬 도메인에 대해 nslookup을 수행할 때 VPN 프로파일 내에 구성된 DNS 서버에서 처리하는 DNS 요청이 10.x 주소로 올바르게 확인됩니다. 또한 비보안 경로에서 확인된 IP(예: 10.59.130.193)로 라우팅 테이블이 업데이트되었습니다.
  - 비작동 시나리오 - 그러나 VPN 프로필에 정의된 DNS 서버 대신 untun4 및 en0 어댑터에 구성된 macOS 시스템의 로컬 DNS(192.168.x.x)에서 동일한 DNS 요청을 처리하면 문제가 발생하는 동안 패킷 캡처에서 이러한 동작이 명확하게 관찰되었습니다.
  - 개인 도메인이 IP 범위 34.x.x.x로 해결되어 연결 문제가 발생했습니다. Wireshark 캡처는 이 문제의 근본 원인을 파악하는 데 도움이 되었습니다.
- 설계 및 컨피그레이션의 관점에서 스플릿 터널 VPN 프로파일 설정의 경우 로컬 시스템 DNS/기본 DNS에 의존하지 않고 스플릿 DNS를 사용하는 것이 좋습니다.
- 또한 이 EKS 클러스터의 트래픽이 원격 터널 인터페이스를 통해 올바르게 조정되도록 us-east-eks-amazonaws.com 항목이 추가되었습니다.
- 또한 RAVPN 인터페이스는 Umbrella 모듈보다 우선해야 하며 Umbrella Organization ID가 포함된 OrgInfo.json 파일과 충돌해서는 안 된다는 내용도 설명했습니다.
- 트러블슈팅 프로세스 동안 Umbrella 모듈이 없는 CSC 클라이언트를 새로 설치했습니다. 이 시나리오에서는 문제를 확인할 수 없었습니다. Umbrella의 관점에서도 내부 도메인 목록에 구성된 루트 도메인 naic.org를 검토하여 Umbrella를 우회할 수 있었습니다. 이는 로컬 도메인 확인이 커널 레벨 루프백 인터페이스에서 Umbrella DNS 모듈에 의해 가로채지지 않은 macOS 구성 시스템 DNS로 전달됨을 의미합니다.

이는 Umbrella 모듈이 없을 때 발생하는 문제를 해결하는 것과 관련이 있습니다. 트래픽 조정 규칙의 올바른 도메인과 스플릿 DNS 구성을 포함한 올바른 VPN 프로필 구성을 사용하면 Umbrella 모델이 켜져 있더라도 문제가 발생하지 않아야 합니다.

사용자가 DNS 모드를 스플릿 터널로 수정하고 VPN 프로필 컨피그레이션을 편집한 후 문제가 해결되었음을 확인했습니다.

원인

VPN 프로필 - 보안 액세스 우회 - DNS 모드는 스플릿 터널로 설정되어야 하며(사용 사례 시나리오에서 가장 일반적으로 나타나는 옵션), 모든 개인/내부 애플리케이션 도메인을 스플릿 DNS 컨피그레이션에 포함시켜 문제를 해결합니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.